In the Specification

Please amend the paragraph beginning at Page 8, Line 15 as follows:

The first line of defense is the ability to tightly control the level of access and the electronic processes relied upon in the major elements of the system and to the information stored within the system. This authentication process is carried out from a client workstation to the reception zone 12. Through a public key infrastructure (PKI), users and the processes relied upon (i.e., client to server, etc) mutually authenticate one another. The resulting session is encrypted and all transactions signed. Access to the PKI certificates is further controlled by the access control list of the X.500 directory ~~102 (see Figure 4)~~ resident in a server 18 of the reception zone 12. By restricting access to the X.500 entries, a more granular need-to-know policy is enforced.

Please amend the paragraph beginning at Page 12, Line 9 as follows:

The public key infrastructure (PKI) is controlled and managed by a certificate authority (CA) 104 resident in server 32. The CA 104 is responsible for all aspects of certificate management. This is coordinated and supported through the PKI Proxy server 110 and PKI client residing on the desktop of the user. These client side applications coordinate all PKI related management tasks with the CA 104. These transactions are encrypted and signed to ensure confidentiality and integrity. Information on the certificates themselves are stored within an X.500 directory ~~102~~ resident in a server 34. This directory is accessed by PKI enabled components such as the PKI Proxy client 108 to obtain the encryption and signature keys of the peer server component. Access to the directory server is performed through authentication.

Please amend the paragraph beginning at Page 13, Line 26 as follows:

The server 34 hosts the primary X.500 directory ~~102~~. The directory contains a master set of X.509 certificates for all valid system users. Automated synchronization software ensures that the X.500 directory 102 located in the reception zone 12 on the server 18 is always current with the master in the operations zone 14.

Please amend the paragraph beginning at Page 30, Line 10 as follows:

Referring to FIGURES ~~6A, 6B and 6C~~ 4A, 4B and 4C, there is illustrated a high level abstraction (flowchart) of the security filtering algorithm for the management system of FIGURE 1. Initially, the user's ID is obtain at an operation 59, an inquiry 61 determines if there are more secure documents to process. If the inquiry is a positive response, then the algorithm proceeds as follows. The algorithm initializes clearance and caveat access at 63.